UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF TENNESSEE
NASHVILLE DIVISION

UNITED STATES OF AMERICA	)	
	)	**No. 3:24-CR-00151**
v.	)	**JUGDE RICHARDSON**
	)	
MATTHEW ISSAC KNOOT	)	

MOTION TO SUPPRESS

Matthew Knoot, through counsel, and pursuant to the Fourth Amendment, moves to suppress all evidence that law enforcement discovered on any device found in his apartment—along with all information that it received from Discord, Inc.—because those devices (and the Discord data) were searched and seized pursuant to facially invalid warrants.

As shown below, the warrant authorizing the search of "any digital devices" (the "Device Warrant") is defective because: (1) it allowed law enforcement to review and make copies of *all* data found on *any* device discovered in Knoot's apartment, irrespective of whether the device (or data) has or had anything to do with the crimes under investigation (a particularity problem), and (2) the affidavit submitted in support of it lacks case-specific facts demonstrating why law enforcement expected to find evidence on Knoot's personal devices (i.e., a nexus problem).

And the warrants permitting law enforcement to access records from Discord (the "Discord Warrants") are also intolerable because: (1) law enforcement relied on tainted information (namely, information discovered via the illegal search of Knoot's computer) to procure it (a poisonous-tree problem), and (2) like the Device Warrant, it authorized law enforcement to indiscriminately access every inch of data associated with Knoot's Discord account—including, for instance, private messages bearing no relevance to criminal behavior and which were sent or received long before law enforcement even suspected that Knoot had committed a crime.

Under these circumstances, this Court should suppress all evidence that law enforcement discovered by way of the Device Warrant and the Discord Warrants. *United States v. Brown*, 828 F.3d 375, 382 (6th Cir. 2016) (affirming suppression when warrant affidavit failed to establish a nexus between the thing to be searched and the crime under investigation); *United States v. Ramirez*, 180 F. Supp. 3d 491, 493 (W.D. Ky. 2016) (affirming suppression of evidence obtained from digital device when affidavit submitted in support of device warrant failed to establish a nexus between the device and the crime and otherwise lacked particularity).

BACKGROUND

1. On April 4, 2023, a company operating in the United States informed the FBI that one of its remote IT workers was using a Virtual Private Network (VPN) to connect a company-issued laptop to a Chinese Internet Protocol (IP) address. (**Ex. A**, Device Warrant, ¶¶ 15-17).

Suspecting some type of computer crime, the FBI interviewed the employee in question—referred to as "A.M."—and learned that A.M. did not work for the company; this, in turn, led the FBI to believe that A.M.'s identity had been stolen and used to get the IT job. (*Id.*, ¶¶ 17-18).

The FBI later learned that A.M.'s identity (i.e., his name and social security number) had been used to secure remote IT work with two other companies. (*Id.*, ¶¶ 19-20).

All three companies advised the FBI that they "shipped company laptops to 1818 Church Street, Apartment 103 in Nashville, Tennessee after hiring [the] individual they believed was" A.M., so the FBI subpoenaed the property management company that operates those apartments and learned that Matthew Knoot occupied Apartment 103. (*Id.*, ¶¶ 20-21).

At that point, the FBI suspected that Knoot or someone else residing in Knoot's apartment had committed identity theft (by using A.M.'s identity to secure the company-issued laptops) and

some form of computer fraud (by accessing the company-issued laptops without authorization or under false pretenses), in violation of 18 U.S.C. §§ 1028 and 1030. (*Id.*, ¶ 7).

2. On August 2, 2023, FBI Agent Derek Rosseau applied for a warrant to search Apartment 416[1] (and Knoot's storage unit) for digital devices—such as cellphones, computers, laptops, tablets, PDAs, pagers, beepers, digital cameras, printers, scanners, hard drives, floppy disks, flash drives, memory cards, and tapes (but not VHS tapes)—and to seize those devices, make copies of any media or information electronically stored on them, and then review that electronic data to see if any of it might qualify as evidence of criminal activity. (*Id.*, ¶ 25).

In applying for the Device Warrant, Agent Rosseau acknowledged that he didn't know whether the FBI would find any devices in Apartment 416 (or the storage unit) but submitted that, "if digital devices are found" during the search, then "there is probable cause to believe that evidence, fruits, and instrumentalities . . . crime" will be found on them. (*Id.*, ¶¶ 26, 32).

This is because, Agent Rosseau explained, his "training and experience" has taught him that people suspected of committing identity theft or computer fraud "use digital devices" to "communicate with co-conspirators" (either via text message or phone call). (*Id.*, ¶¶ 24, 26).

Notably, however, nothing in Agent Rosseau's affidavit indicates that more than one person was involved in the crimes under investigation (which takes the wind out of his claim that he expected to find co-conspirator communications on whatever devices were found).

And equally important, the affidavit lacks case-specific facts establishing why Agent Rosseau believed that any digital devices that might be found in Apartment 416 (beyond the company-issued laptops, of course) would contain evidence of the crimes under investigation.

[1] On July 7, 2023, the company that manages the Church Street apartments notified the FBI that Knoot had relocated to Apartment 416 and that Knoot was also "renting storage unit #2). (*Id.*, ¶ 23).

Notwithstanding these defects, the magistrate judge granted Agent Rosseau's warrant application at 3:48 p.m. on August 2, 2023 (i.e., the same day he applied for it). (*Id.*, pg. 23).

3. On August 8, 2023, the FBI executed the Device Warrant and, during their search of Apartment 416, they found Knoot's: (1) a personal, custom desktop computer, and (2) cellphone. Presumably, they also found the above-referenced company-issued laptops.

The FBI later searched Knoot's personal computer and phone and, in the process, discovered two Microsoft Word documents: one titled "yanddi0027 setup terms.docx" and the other labeled "setupconversation.docx." (*See* **Ex. B**, Discord Warrant, ¶ 16).

These documents contained what "appeared to be partial conversations" between two Discord users—one with username "mellamomateo," the other "yangdi0027"—"discussing [a] remote IT work scheme."[2] (*Id.*, ¶ 16). In the messages, the user known as "yangdi0027" explained that he was going to send laptop computers to "mellamomateo" and that "mellamomateo" would be paid simply to plug those computers in and connect them to the Internet. (*Id.*).

It's unclear what motivated the FBI to open these documents, and, notably, nothing in the Device Warrant expressly authorized the FBI to search Microsoft Word files (instead, as mentioned, it apparently authorized law enforcement to review all stored data).

4. On April 22, 2024, FBI Agent Rosseau applied for two warrants pursuant to which it commanded Discord, Inc. to "disclose to the government" several categories of information related to the "mellamomateao" and "yangdi0027" accounts, including: (1) all registration information, (2) "IP logs and other documents showing . . . each login to the account from account creation to present," (3) "[a]ll data and information associated with the profile page" for the accounts, "including photographs, 'bios,' and profile background and themes," (4) "[a]ll privacy and account

[2] Discord is a free app that allows users to communicate with each other three text, voice, and video.

settings," (5) "[a]ll log data, including browser type, operating system, referring web pages, pages visited, location, mobile carrier, device and application IDs, search terms and cookie information from account creation to present," and (6) "[a] listing of any and all groups, guilds, or servers that the user administers or is a part of." (*See* **Ex. B**, Discord Warrant, pg. 28-29).

The warrants also requested "[a]ny and all private messages, instant message or direct message sent or received"—along with date and timestamps—irrespective of when the messages were sent or who the messages were sent to or received from. (*Id.*, pg. 29).

5. On August 7, 2024, the Government used the fruits of the aforementioned searches (i.e., the device search and the Discord search) to indict Knoot for: (1) conspiring to cause damage to protected computers, (2) conspiring to commit money laundering, (3) conspiring to commit wire fraud, (4) intentionally damaging a protected computer, (5) aggravated identity theft, and (6) conspiring to cause the unlawful employment of aliens. (DE 3, Indictment, PageID #7-16).

As explained below, however, the fruits of those searches—that is, the data discovered on devices found in Knoot's apartment (and the materials received from Discord)—should be suppressed because the warrants authorizing the discovery of those fruits are facially invalid.

LAW & ARGUMENT

The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects" by requiring the Government to obtain a valid, judge-approved warrant prior to searching or seizing a person, place or thing. U.S. Const. amend. IV.; *Riley v. California,* 573 U.S. 373, 382 (2014) (providing that "where a search is undertaken by law enforcement to discovery evidence of criminal wrongdoing," the Fourth Amendment "generally requires" the Government to first obtain a "judicial warrant" (cleaned up) (citation omitted)).

To be valid, the warrant must be supported by probable cause, probable cause must be shown by way of by an affidavit ("Oath or Affirmation"), and the affidavit, in turn, must: (1) contain case-specific facts establishing a "nexus" between the place or thing to be searched or seized and the crimes under investigation, and (2) be free of "tainted" (i.e., illegal obtained) information. *United States v. Brown,* 828 F.3d 375, 382 (6th Cir. 2016) (discussing the nexus requirement); *see also Murray v. United States*, 487 U.S. 533, 540 (1988) (explaining that law enforcement cannot use information learned via an illegal search to obtain a warrant).

The warrant must also "particularly describe[] the place to be searched[] and the persons or things to be seized," U.S. Const. amend. IV—indeed, a warrant with "indiscriminate sweep is constitutionally intolerable." *United States v. Griffith*, 867 F.3d 1265, 1275 (D.C. Cir. 2017).

Each of these requirements—probable cause, nexus, particularity—represent "the founding generation's response to the reviled 'general warrants' and 'writs of assistance' of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity." *Riley*, 573 U.S. at 403; *United States v. Sanchez,* 509 F.2d 886, 889 (6th Cir. 1975) (the Fourth Amendment was "designed to eliminate the pernicious general warrant").

And each requirement is important. Failure to satisfy even just one generally renders the warrant invalid and any evidence obtained pursuant to it inadmissible. *See, e.g.*, *Brown,* 828 F.3d at 382 (addressing a "nexus" problem and observing: "If the affidavit does not present sufficient facts demonstrating why the police officer expects to find evidence in the [place to be searched] rather than in some other place, a judgment not find probable cause to issue a search warrant.").

Here, the Government obtained several warrants—the Device Warrant (so that it could search any device found in Apartment 416) and the Discord Warrant(s) (because it wanted records related to Knoot's Discord account)—but none comply with the Fourth Amendment.

A. The Device Warrant Defies the Fourth Amendment

Start with the Device Warrant. Under it, the Government asked for (and received) permission to search Knoot's apartment and storage unit for any and all "digital devices"—including personal devices—and to seize those devices and then review and search through every inch of data stored on them for evidence of computer fraud or identity theft.

But does the warrant identity with particularity the place to be searched and the items to be seized? And does the affidavit that Agent Rosseau submitted in support of it contain a "substantial [factual] basis" from which the issuing magistrate could conclude that law enforcement had probable cause to believe that evidence of crime would be found on digital devices *other* than the company-issued laptops—such as, for instance, Knoot's personal devices? *Brown*, 828 at 381 (citation omitted) (judge must have "substantial basis for concluding that probable cause existed").

The answer to both questions is no. Thus, the Government violated the Fourth Amendment when it seized Knoot's personal devices and indiscriminately searched all data stored on them.

1. The Device Warrant lacks particularity.

The Fourth Amendment requires that warrants "particularly describ[e] the place to be searched[] and the persons or things to be seized." U.S. Const. amend. IV; *Stanford v. State of Texas*, 379 U.S. 476, 486 (1965) (overbroad warrants are "constitutionally intolerable").

And this key requirement is even "more important" in situations involving searches and seizures of digital devices. *United States v. Otero*, 563 F.3d 1127, 1132 (10th Cir. 2009).

This is because digital devices can "store and intermingle a huge array of one's personal papers in a single place," which, in turn, "increases" the likelihood that law enforcement will inappropriately intrude on the privacies of one's life. *Id.*; *Riley*, 573 U.S. at 403.

To that end, "warrants for [device] searches must *affirmatively limit* the search to the evidence of specific federal crimes or specific types of material." *Otero*, 563 F.3d at 1132.

In other words, a device warrant must: (1) specifically identify *which* devices are subject to search-and-seizure, *see, e.g.*, *Griffith*, 867 F.3d at 1275-76, and (2) "identify" the information on the device that is subject to review, *Otero*, 563 F.3d at 1132; Office of Legal Educ., *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, Crim. Div., Dep't of Justice 69-72 (2015) (explaining that, "[w]hen probable cause to search relates in whole or in part to information stored on a computer . . . the warrant should identify that information with particularity, focusing on the content of the relevant files rather than the . . . devices").

Here, the Device Warrant fails both tests. Attachment A to the Device Warrant does not identify with particularity which "digital devices" are subject to seizure but says instead that law enforcement can seize any "digital device" found in Apartment 416. (**Ex. A**, Device Warrant, pg. 25). And Attachment B simply says that "items, information, and data" that law enforcement can seize and review includes ("*but [is] not limited to*") the data "described in the warrant" and "media" or "information" stored on the seized devices. (*Id.*, pg. 26-27).

In other words, the Device Warrant apparently authorized law enforcement to seize any "device" found at Apartment 416 or the storage unit—including (but not limited to) cellphones, computers, laptops, tablets, PDAs, pagers, beepers, digital cameras, printers, scanners, hard drives, floppy disks, flash drives, and memory cards—and to search and make copies of any "media," "information," or "data" found on them, just in case any such "media," "information," or "data" turned out to be "fruits, evidence, [or] contraband." (*Id.*, ¶ 25, pg. 25-27).

In this way, the Device Warrant lacks particularity and is therefore overbroad and invalid. *See, e.g.*, *Otero*, 563 F.3d at 1132 (holding that warrant authorizing the search of a computer was

"invalid" for lack of particularity because it appeared to allow law enforcement to search "any and all information and/or data" stored on the computer); *see also State v. Castagnola*, 46 N.E. 3d 638, 656-57 (Ohio 2015) (concluding that warrant authorizing a review of any "records and documents stored on" a certain computer lacked particularity and was thus invalid).

Thus, all evidence seized pursuant to it should be excluded. *Brown*, 828 F.3d at 385 ("When evidence is obtained in violation of the Fourth Amendment," the typical remedy is suppression. (citation omitted)); *Castagnola*, 46 N.E. 3d at 659-70 (concluding that all information obtained pursuant to overbroad warrant should be suppressed).

2. The warrant affidavit lacks facts sufficient to establish a nexus between Knoot's personal devices and the crimes under investigation.

Issues of particularity aside, the Device Warrant is also constitutionally infirm insofar as it authorized law enforcement to seize and search Knoot's *personal* devices.

Agent Rosseau didn't say much about the relationship between Knoot's personal devices and the crimes under investigation in the warrant-affidavit. He did not, for instance, attest to any case-specific facts suggesting that Knoot's personal devices were used in connection with a crime. (**Ex. A**, Device Warrant, ¶¶ 16-23). Nor did he include a case-specific explanation for why he thought those devices (if present) would contain evidence of wrongdoing.[3]

Rather, all Agent Rosseau said was that, *if* Knoot has personal devices, then "there is probable cause to believe" that those devices will contain evidence of crime because his "training and experience" has taught him that "[i]ndividuals" suspected of identity theft or computer fraud "use digital devices," including personal ones, to facilitate illegal activity. (*Id.*, ¶¶ 24, 26).

[3] Recall that Agent Rosseau expressly acknowledged that he did not know whether law enforcement would even find personal digital devices in the apartment, (*id.*, ¶ 26)—thus, not only did Agent Rosseau fail to explain why he thought Knoot's personal devices constituted instrumentalities of crime or contained evidence, but he apparently did not even know whether those devices existed, much less that such devices would be found in the apartment.

And this boilerplate "training-and-experience" attestation is far too "vague" and "generalized" to establish a "direct connection" between Knoot's personal computer and cellphone and the crimes under investigation. *See Brown*, 828 F.3d at 382 (explaining that nexus-facts "must be specific and concrete, not 'vague' or 'generalized'"); *see also Illinois v. Gates*, 462 U.S. 213, 239 (1983) (observing that a "conclusory statement" cannot support a finding of probable cause).

a. *Schultz*—a Sixth Circuit case discussing the issues with "training-and-experience" allegations in warrant-affidavits—helps show why. There, an agent investigating a drug dealer learned that the dealer "maintained safe deposit boxes" at a particular bank, so he sought a warrant to searches those boxes. *United States v. Schultz*, 14 F.3d 1093, 1096 (6th Cir. 1994). The reason? "Based on his training and experience, [he] believe[d] . . . that [suspected drug dealers keep] records, etc. of [drug] distribution . . . in bank safe deposit boxes." *Id.* at 1097. A magistrate later issued a warrant, and the agent searched the deposit boxes and found (what he believed to be) evidence of crime, and that evidence was used to prosecute him for drug dealing. *Id.* at 1096. On appeal, the drug dealer argued that the agent violated the Fourth Amendment when he (the agent) searched his (the drug dealer's) deposit boxes, claiming that the agent did not offer any case-specific explanation for why he believed the boxes contained evidence of crime. *Id.* at 1097. And the Sixth Circuit agreed, reasoning that, although "an officer's 'training and experience' may be considered in determining probable cause[,] it [was] []not [a] substitute for the lack of evidentiary nexus" between the crime under investigation and the deposit boxes because the agent "did not have anything more than a guess that contraband or evidence would be found in the boxes." *Id.* at 1097-98. To hold otherwise, the court concluded, "would be to invite general warrants authorizing searches of *any* property owned, rented, or otherwise used by a criminal suspect—just the type of broad warrant the Fourth Amendment was designed to foreclose." *Id.* at 1098.

Here, as in *Schultz*, Agent Rosseau's warrant affidavit does not contain any case-specific facts establishing a "material connection" between Knoot's devices and criminal activity, which, in turn, shows that Agent Rosseau's claim that Knoot's devices (if any) might contain evidence of crime was nothing "more than a guess." *See Schultz*, 14 F.3d at 1097-98.

Thus, as in *Schultz*, Agent Rosseau's allegation that his "training and experience" has taught him that "[i]ndividuals who engage in criminal activity" may use personal devices (like computers or cellphones) to further that activity does not establish an evidentiary nexus between Knoot's personal devices and the crimes under investigation. (**Ex. A**, Device Warrant, ¶ 26).

The result? Law enforcement violated the Fourth Amendment when they searched and seized Knoot's personal devices. *See Schultz*, 14 F.3d at 1097-98; *United States v. Ramirez*, 180 F. Supp. 3d 491, 495 (W.D. Ky. 2016) (concluding that warrant-affidavit failed to establish a nexus between defendant's cellphone and his crime-of-arrest when the only information in the affidavit about the connection between the two was a "training and experience" allegation).

b. The Government may argue that *Schultz* is distinguishable because it involved an object (a box) whereas this case involves digital devices (a personal computer and a cellphone).

But that distinction does help the Government. Several courts—some federal, others state—have applied the principles underlying *Schultz* to hold that law enforcement cannot seize and search a suspect's cellphone or computer simply because their "training and experience" tells them that suspects occasionally use those devices in connection with crime. *See, e.g.*, *Ramirez*, 180 F. Supp. 3d at 495; *State v. Baldwin*, 664 S.W.3d 122 (Tex. Crim. App. 2022); *Buckham v. State*, 185 A.3d 1 (Del. 2018); *Commonwealth v. White*, 59 N.E. 3d 369 (Mass. 2016).

Ramirez is an example. There, law enforcement arrested a suspected drug dealer and found a cellphone in his pocket during a search-incident-to-arrest. *Ramirez*, 180 F. Supp. 3d at 492-93.

Apparently aware that the Supreme Court's decision in *Riley v. California* prohibited her from searching the suspect's cellphone incident to arrest, the arresting officer applied for a warrant so that law enforcement could "forensically examine[] . . . all personal files and information stored [on] the cell phone." *Ramirez*, 180 F. Supp. 3d at 493. She said she had probable cause to believe that evidence of crime would be on the phone because her "training and field experience" taught her" that individuals keep text messages and other electronic information stored in their cell phones which may relate them to crime and/or co-defendants/victims." *Id.* A state-court judge issued the warrant, but, when the Government tried to use evidence taken from the phone to bring federal charges, the defendant moved to suppress, and the district court granted his motion. *Id.* at 496. In doing so, the district court explained that the officer's "training and experience" allegation failed to establish a nexus between the crimes under investigation and the defendant's cellphone. *Id.*

And other examples include:

- *State v. Baldwin*, 664 S.W.3d 122, 123 (Tex. Crim. App. 2022) (holding that an officer's attestation that his "training and experience" taught him that suspects frequently use smartphones in furtherance of criminal activity is not by itself sufficient to establish a nexus between a phone and a crime).

- *Commonwealth v. White*, 59 N.E. 3d 369 (Mass. 2016) (concluding that "probable cause to search or seize a person's cellular telephone may not be based solely on an officer's opinion that the device is likely to contain evidence of the crime under investigation")

- *Buckham v. State*, 185 A.3d 1 (Del. 2018) (reasoning that officer's attestation that "criminals often communicate through their cellular phones" was far "too vague and too general to connect" the defendant's phone to the crime under investigation and that, consequently, law enforcement lacked probable cause to search the defendant's phone).

- *State v. Schubert*, 219 N.E.3d 916 (Ohio 2022) (finding that officer's statement that he has learned through his "training and experience" that "digital devices . . . may contain additional evidence" of wrongdoing was insufficient to satisfy the nexus requirement and noting that, despite that allegation, the affidavit lacked "information providing any reason to believe that" the device "would contain evidence").

These outcomes make sense. Digital devices are "not inherently illegal" and will often (if not always) store personal information that has nothing to do with crime. *Griffith*, 867 F.3d at 1274; *Riley*, 573 U.S. at 394 (discussing storage capacity of digital devices). Thus, device searches will often (if not always) implicate privacy concerns that simply don't exist in the physical world. *Riley*, 573 U.S. at 394. And in this way, the nexus-requirement is all the more important when it comes to searches of digital devices. *Griffith*, 867 F.3d at 1274 (law enforcement must explain why they "believe that a [device] contain[s] evidence of . . . crime" before searching it).

So again, by seizing and searching Knoot's personal computer and cellphone without first establishing (with specific and concrete facts) that those devices had anything to do with the crimes under investigation, the Government violated Knoot's Fourth Amendment rights.

c. A final point about the nexus requirement. Even if this Court concludes that law enforcement can satisfy the nexus requirement with nothing more than an officer's statement that his "training and experience" has led him to believe that digital devices contain evidence of crime, Agent Rosseau's affidavit still does not justify the search or seizure of Knoot's personal devices.

Agent Rosseau attested that his "knowledge, training, and experience" led him to believe that—"*if* digital devices [were] found" in Apartment 416—then those devices would contain evidence of crime because suspects use devices "to communicate with co-conspirators online" and to store information related to co-conspirators." (**Ex.** A, Device Warrant, ¶ 26).

But Agent Rosseau was not investigating a conspiracy, and nothing in the warrant-affidavit suggests Agent Rosseau suspected that more than one person was involved in committing the "acts under investigation," (*Id.*, ¶¶ 16-23)—indeed, Agent Rosseau did not even attest that his "training and experience" has taught him that most criminals enlist help from others.

It follows that, even if an officer's "training and experience" about how suspects use their personal digital devices to communicate with accomplices is sufficient to justify the search of a suspect's device in the mine run of cases, Agent Rosseau's allegation does little work here because he provided no explanation for his belief that Knoot (or whoever else he suspected) had conspired with others to commit the crimes under investigation.

In sum: Agent Rosseau applied for a warrant to seize and search any device found in Apartment 416 because his "training and experience" taught him that devices *might* be present, (*id*, ¶ 24), and that, since "[i]ndividuals who engage in criminal activity" sometimes use their phones to communicate with co-conspirators," (*id.*, ¶ 26), those devices—*if present*—"might" contain "evidence" of crime," (*id.*, ¶ 25). That allegation falls far short of establishing a "material connection" between Knoot's personal devices and the crimes under investigation. *See Schultz*, 14 F.3d at 1097. Thus, Agent Roseau's affidavit did not provide probable cause to search and seize those devices, the warrant allowing a search and seizure of those devices is invalid, and, by searching and seizing those devices pursuant to an invalid warrant, the Government violated Knoot's Fourth Amendment rights. *See Brown*, 828 F.3d at 384-85.

* * *

In light of the above, the Device Warrant doesn't comply with the probable cause, nexus, and particularity requirements of the Fourth Amendment. It doesn't identify which digital devices (or what data) law enforcement were subject to search-and-seizure. And, with respect to Knoot's personal devices, the affidavit submitted in support of the warrant lacks case-specific facts explaining why law enforcement believed those devices contained evidence. Consequently, all evidence obtained from the devices—or, at the very least, evidence from Knoot's personal devices—should be suppressed. *See, e.g.*, *Brown*, 828 F.3d at 385.

B. The Discord Warrants are Constitutionally Infirm

Through the Discord Warrants, the Government sought and obtained substantial information about Knoot's Discord account (and the Discord account of a co-conspirator that law enforcement learned about through information extracted from Knoot's personal computer) and also gained access to any and all communications that Knoot had ever sent via Discord.

Do the Discord Warrants comply with the Fourth Amendment? The answer is no for a variety of reasons. Thus, all evidence the Government received by way of the Discord Warrants should be suppressed. *United States v. Abernathy*, 843 F.3d 243, 251 (6th Cir. 2016) (suppressing all evidence law enforcement obtained pursuant to an invalid warrant).

1. An initial problem with the Discord Warrants is that the Government relied on tainted information to establish that probable cause supported the issuance of those warrants.

To put this in context: Prior to illegally searching Knoot's personal computer pursuant to the invalid Device Warrant, law enforcement did not know (and apparently did not suspect) that multiple persons working together might have committed the acts under investigation. Rather, it was only *after* law enforcement searched Knoot's personal computer and found Microsoft Word documents containing excerpts from what "appeared to be partial conversations" between two Discord users—namely, "mallamomateao" and "yangdi0027"—that they had reason to believe: (1) that the crimes under investigation had more than one culprit, and (2) that Discord might have information relevant to the investigation. (**Ex. B**, Discord Warrant, ¶ 16). And it was only because of those Word documents that law enforcement was able to establish probable cause in support of the Discord Warrants—indeed, as the affidavits submitted in support of the Discord Warrants show, without the Word documents found on Knoot's personal computer, law enforcement would not have had probable cause to obtain information related to Knoot's Discord account. (*Id.*).

In this way, the Discord Warrants are based on tainted information—namely, information learned from law enforcement's illegal search of Knoot's personal computer—and, without that information, there's nothing left to support the issuance of the Discord Warrants.

Consequently, the Discord Warrants are invalid, and any evidence obtained pursuant to them should be suppressed. *United States v. Smith*, 730 F.2d 1052, 1056 (6th Cir. 1984) (explaining that, "when a search warrant is based partially on tainted evidence" and that "tainted information [is] so important that probable cause [does] not exist without out," the warrant is invalid, and any evidence obtained pursuant to it should be suppressed); *see also Murray v. United States*, 487 U.S. 533, 540 (1988) (tainted information cannot be used to establish probable cause).

2. A second problem with the Discord Warrants is that, like the Device Warrant, they lack particularity U.S. Const. amend. IV (warrant must "particularly describe[e] the place to be searched[] and the persons or things to be seized"); *Stanford*, 379 U.S. at 486.

Through the Discord Warrants, the Government requested disclosure of virtually every kind of data that could be found in (or in relation to) a Discord account, including: (1) "[a]ny and all private messages, instant message or direct message sent or received," (2) all registration information, (3) "IP logs and other documents showing . . . each login to the account from account creation to present," (4) "[a]ll data and information associated with the profile page" for the accounts, "including photographs, 'bios,' and profile background and themes," (5) "[a]ll privacy and account settings," (6) "[a]ll log data, including browser type, operating system, referring web pages, pages visited, location, mobile carrier, device and application IDs, search terms and cookie information from account creation to present," and (7) "[a] listing of any and all groups, guilds, or servers that the user administers or is a part of." (*See* **Ex. B**, Discord Warrant, pg. 28-29).

It's difficult to see how some of these categories of information relate to the crimes under investigation, and, for the categories that make sense—such as the request for private messages—the warrant is unnecessarily overbroad: For instance, if the Government's theory (based on the Word documents extracted from Knoot's personal computer) is that "mallamomateao" and "yangdi0027" conspired to commit computer fraud and identity theft, why does the Government need "[a]ny and all private messages . . . sent or received" from their accounts, regardless of *when* the message was sent or received or *who* the message was sent to or received from?

In this way, the Discord Warrants lack particularity, and all information seized from them should be suppressed. *United States v. Mercery*, 591 F. Supp. 3d 1369, 1381 (M.D. Ga. 2022).

The Middle District of Georgia's decision in *Mercery* underscores this result. There, the Government obtained a warrant requiring Instagram to disclose a substantial amount of data associated with a particular account, including "all data and information associated with [the account's] profile page," "every [IP] address [the account holder] has ever logged in from," "every photograph and image on the account," "all account setting and cookie data," and "every communication between Instagram and any person 'regarding' [the account holder] or his account." *Id.* at 1381. The account holder challenged the warrant on particularity grounds and won because, as the district court put it: "The compelled disclosure is not tailored to evidence of the crimes under investigation, the time period during which [the account holder] allegedly committed the crimes, or the persons allegedly involved in the crimes." *Id.* at 1381-82. In other words, "the warrant amount[ed] to a general rummage of [the account holder's] entire Instagram account," and, since it would have been easy for law enforcement to describe the information sought more particularity, the district court suppressed all evidence obtained via the warrant. *Id.*

Here, as in *Mercery*, the Discord Warrants required Discord "to disclose virtually every type of data associated with" the Discord accounts in question, *see id.* at 1381; thus, as in *Mercery*, the Discord Warrants are overbroad and the fruits of them should be suppressed.

CONCLUSION

In light of the foregoing, the Device Warrant and the Discord Warrants are invalid. The Device Warrant fails to establish a nexus between the acts under investigation and Knoot's personal devices, the Discord Warrant is based on tainted information, and both warrants lack particularity. As a result, all evidence obtained via these warrants should be suppressed.

Respectfully submitted,

s/ *David Fletcher*
DAVID FLETCHER
Assistant Federal Public Defender
810 Broadway, Suite 200
Nashville, Tennessee 37203
615-695-6951
David_fletcher@fd.org

Attorney for Matthew Knoot

CERTIFICATE OF SERVICE

I hereby certify that on April 1, 2025, I electronically filed the foregoing *Motion to Suppress* with the U.S. District Court Clerk by using the CM/ECF system, which will send a Notice of Electronic Filing to the following: Josh Kurtzman, Assistant United States Attorney, 719 Church Street, Suite 3300, Nashville, Tennessee, 37203.